CLAIMS

What is claimed is:

1. An IP Packet Access Gateway (IP PAG) system for managing an IP bearer path between IP endpoints, comprising:

an IP PAG;

a first IP bearer connection termination in said IP PAG for terminating a first bearer connection with a first IP endpoint;

a second IP connection termination in said IP PAG for terminating a second bearer connection with a second IP endpoint;

a call control entity associated with said IP PAG for communicating call control instructions to said IP PAG, said call control instructions including instructions for logically concatenating said connections into an active IP bearer path extending between said first IP endpoint and said second IP endpoint; and

a bearer traffic IP packet handler in said IP PAG for moving bearer traffic IP packet payloads over said active IP bearer path, said packet payloads comprising voice, data, multimedia or other information.

2. A system in accordance with Claim 1 wherein said IP PAG includes a bearer connection address table that associates said active IP bearer path with said first bearer connection and said second bearer connection in accordance with said concatenating instructions.

3. A system in accordance with Claim 2 wherein said connection address table includes a key entry corresponding to said active IP bearer path (IP bearer path entry), and comprising first and second tuples respectively corresponding to said first bearer connection and said second bearer connection.

4. A system in accordance with Claim 3 wherein said first tuple includes a first IP address and a port number for said IP PAG and an IP address and a port number for said first IP endpoint, and said second tuple includes a second IP address

and a port number for said IP PAG and an IP address and a port number for said second IP endpoint.

5. A system in accordance with Claim 4 wherein said bearer traffic IP packet handler is adapted to move bearer traffic IP packet payloads from said first IP endpoint to said second IP endpoint by:

receiving a bearer traffic IP packet from said first IP endpoint over said first bearer connection;

searching for an IP bearer path entry in said connection address table having an associated first tuple that contains the packet header source IP address and source port number of said received IP packet;

upon locating said IP bearer path entry in said connection address table, determining from the second tuple associated with said entry the IP address and port number of said second IP endpoint;

rewriting the packet header of said bearer traffic IP packet using the IP address and port number of said IP PAG as the source IP address and source port number, and using the IP address and port number of said second IP endpoint as the destination IP address and destination port number; and

sending said rewritten bearer traffic IP packet to said second IP endpoint over said second bearer connection.

6. A system in accordance with Claim 5 wherein said bearer traffic IP packet handler is adapted to perform bearer traffic policing to verify that said received bearer traffic IP packet is associated with an active IP bearer path and is authorized for transmission on that path.

7. A system in accordance with Claim 6 wherein each IP bearer path entry in said address connection table includes a status flag indicative of an associated IP bearer path being active or inactive, and wherein said bearer traffic policing includes checking said status flag for active status.

8. A system in accordance with Claim 7 wherein said bearer traffic policing includes logging and/or dropping unauthorized packets.

9. A system in accordance with Claim 7 wherein said connection address table contains multiple IP bearer path entries having associated tuples identifying said first IP endpoint, and wherein said IP PAG is controllable by said call control entity to act as a IP bearer path pivot point by selectively activating the status flags associated with said IP bearer path entries.

10. A system in accordance with Claim 1 further including a signaling traffic IP packet handler for relaying signaling messages from one or both of said IP endpoints to a destination.

11. A system in accordance with Claim 10 wherein said signaling traffic IP packet handler maintains an IP endpoint address table that lists IP addresses for IP endpoints that are authorized to send signaling messages to said destination, and which lists IP port numbers, one for each of authorized IP endpoint.

12. A system in accordance with Claim 11 wherein said signaling message relay includes receiving a signaling traffic IP packet from said first or second IP endpoint and rewriting the packet header of said signaling packet by:

setting the source IP address to the IP address of said IP PAG;

setting the source port number to an IP port of said IP PAG as determined from said IP endpoint address table;

setting the destination IP address to an IP address of said destination as determined by the source IP address and the destination port number of the signaling message received; and

leaving the destination IP port unchanged.

13. A system in accordance with Claim 12 wherein said signaling message is an H.323, SIP, or H.248 signaling message and said destination is a call control entity.

14. A system in accordance with Claim 12 wherein said signaling message is an SNMP signaling message and said destination is an SNMP manager.

15. A system in accordance with Claim 12 wherein said signaling traffic IP packet handler is adapted to perform signaling traffic policing to verify that said IP endpoint sending said signaling messages is authorized to send such messages.

16. A system in accordance with Claim 15 wherein said signaling traffic policing includes performing a table lookup in said IP endpoint address table relative to an IP signaling packet received from said first IP endpoint to verify that said IP endpoint is listed in said table and to obtain a port number assigned to said IP endpoint from said table.

17. A system in accordance with Claim 15 wherein said call control entity is adapted to dynamically throttle signaling messages sent to said destination.

18. A system in accordance with Claim 1 wherein said system includes a line-side IP PAG terminating plural IP lines and a trunk-side IP PAG terminating plural IP trunks.

19. A system in accordance with Claim 18 and further including an IP switching fabric between said line-side IP PAG and said trunk-side IP PAG.

20. A system in accordance with Claim 19 and further including one or more resource servers, interworking gateways, interworking units, or data termination systems.

21. A method for managing an IP bearer path between IP endpoints, comprising the steps of:

terminating a first IP bearer connection with a first IP endpoint;

terminating a second bearer connection with a second IP endpoint;

logically concatenating said connections into an active IP bearer path extending between said first IP endpoint and said second IP endpoint; and

moving bearer traffic IP packet payloads over said active IP bearer path, said packet payloads comprising voice, data, multimedia or other information.

22. A method in accordance with Claim 21 wherein said concatenating step comprises establishing a key entry in a bearer connection address table that associates said active IP bearer path with said first bearer connection and said second bearer connection.

23. A method in accordance with Claim 22 wherein said key entry corresponds to said active IP bearer path (IP bearer path entry) and comprises first and second tuples respectively corresponding to said first bearer connection and said second bearer connection.

24. A method in accordance with Claim 23 wherein said first tuple includes a first IP address and a port number for said IP PAG and an IP address and a port number for said first IP endpoint, and said second tuple includes a second IP address and a port number for said IP PAG and an IP address and a port number for said second IP endpoint.

25. A method in accordance with Claim 24 wherein said moving step includes moving bearer traffic IP packet payloads from said first IP endpoint to said second IP endpoint by:

receiving a bearer traffic IP packet from said first IP endpoint over said first bearer connection;

searching for an IP bearer path entry in said connection address table having an associated first tuple that contains the packet header source IP address and source port number of said received IP packet;

upon locating said IP bearer path entry in said connection address table, determining from the second tuple associated with said entry the IP address and port number of said second IP endpoint;

rewriting the packet header of said bearer traffic IP packet using an IP address and a port number associated with said active bearer path as the source IP address and source port number, and using the IP address and port number of said second IP endpoint as the destination IP address and destination port number; and

sending said rewritten bearer traffic IP packet to said second IP endpoint over said second bearer connection.

26. A method in accordance with Claim 25 further including performing bearer traffic policing to verify that said received bearer traffic IP packet is associated with an active IP bearer path and is authorized for transmission on that path.

27. A method in accordance with Claim 26 wherein each VoIP bearer path entry in said address connection table includes a status flag indicative of an associated IP bearer path being active or inactive, and wherein said bearer traffic policing step includes checking said status flag for active status.

28. A method in accordance with Claim 27 wherein said bearer traffic policing includes logging and/or dropping unauthorized packets.

29. A method in accordance with Claim 27 wherein said connection address table contains multiple IP bearer path entries having associated tuples identifying said first IP endpoint, and wherein a bearer path pivot point is implemented by selectively activating the status flags associated with said IP bearer path entries.

30. A method in accordance with Claim 21 further including relaying signaling messages from one or both of said IP endpoints to a destination.

31. A method in accordance with Claim 30 wherein said signaling message relaying step includes maintaining an IP endpoint address table that lists IP addresses for IP endpoints that are authorized to send signaling messages to said destination, and which lists IP PAG port numbers, one for each authorized IP endpoint.

32. A method in accordance with Claim 31 wherein said signaling message relay step includes receiving a signaling traffic IP packet from said first IP endpoint and rewriting the packet header of said signaling packet by:

setting the source IP address to IP address of said IP PAG relaying said signaling messages;

setting the source port number to said IP port assigned to said first IP endpoint, as determined from said IP endpoint address table;

setting the destination IP address to an IP address of said destination, as determined by said source IP address and the destination port number of said signaling message received; and

leaving the destination IP port unchanged.

33. A method in accordance with Claim 32 wherein said signaling message is an H.323, SIP, H.248, or other call signaling message and said destination is a call control entity.

34. A method in accordance with Claim 32 wherein said signaling message is an SNMP signaling message and said destination is an SNMP manager.

35. A method in accordance with Claim 32 wherein said signaling message relay step performs signaling traffic policing to verify that said IP endpoint sending said signaling messages is authorized to send such messages.

36. A method in accordance with Claim 35 wherein said signaling traffic policing includes performing a table lookup in said IP endpoint address table relative to an IP signaling packet received from said first IP endpoint to verify that said IP endpoint is listed in said table and to obtain a port number assigned to said first IP endpoint from said table.

37. A method in accordance with Claim 35 further including dynamically throttling signaling messages received at said IP PAG.

38. A method in accordance with Claim 21 including terminating plural IP lines at a set of line-side terminating points and terminating plural IP trunks at a set of trunk-side terminating points.

39. A method in accordance with Claim 38 further including performing switching between said line-side and trunk-side terminating points.

40. A method in accordance with Claim 39 further including connecting one of more of said line-side or trunk side terminating points to one or more resource servers, interworking gateways, interworking units, or data termination systems.

41. A computer program product for managing an IP bearer path between IP endpoints, comprising:

one or more data storage media;

program means recorded on said one or more data storage media for:

terminating a first IP bearer connection with a first IP endpoint;

terminating a second bearer connection with a second IP endpoint;

logically concatenating said first and second bearer connections into an active IP bearer path extending between said first IP endpoint and said second IP endpoint; and

moving bearer traffic IP packet payloads over said active IP bearer path, said packet payloads comprising voice, data, multimedia or other information.

42. A program product in accordance with Claim 41 wherein said concatenating program means comprises program means for establishing a key entry in a bearer connection address table that associates said active IP bearer path with said first bearer connection and said second bearer connection.

43. A program product in accordance with Claim 42 wherein said key entry corresponds to said active IP bearer path (IP bearer path entry) and comprises first and second tuples respectively corresponding to said first bearer connection and said second bearer connection.

44. A program product in accordance with Claim 43 wherein said first tuple includes a first IP address and a port number associated with said IP PAG and an IP address and a port number for said first IP endpoint, and said second tuple includes a second IP address and a port number associated with said IP PAG and an IP address and a port number for said second IP endpoint.

45. A program product in accordance with Claim 44 wherein said moving program means includes program means for moving bearer traffic IP packet payloads from said first IP endpoint to said second IP endpoint by:

receiving a bearer traffic IP packet from said first IP endpoint over said first bearer connection;

searching for an IP bearer path entry in said connection address table having an associated first tuple that contains the packet header source IP address and source port number of said received IP packet;

upon locating said IP bearer path entry in said connection address table, determining from the second tuple associated with said entry the IP address and port number of said second IP endpoint;

rewriting the packet header of said bearer traffic IP packet using an IP address and a port number associated with said active bearer path as the source IP address and source port number, and using the IP address and port number of said second IP endpoint as the destination IP address and destination port number; and

sending said rewritten bearer traffic IP packet to said second IP endpoint over said second bearer connection.

46. A program product in accordance with Claim 45 further including program means for performing bearer traffic policing to verify that said received bearer traffic IP packet is associated with an active IP bearer path and is authorized for transmission on that path.

47. A program product in accordance with Claim 46 wherein each IP bearer path entry in said address connection table includes a status flag indicative of an associated IP bearer path being active or inactive, and wherein said bearer traffic policing step includes checking said status flag for active status.

48. A program product in accordance with Claim 47 wherein said bearer traffic policing program means includes program means for logging and/or dropping unauthorized packets.

49. A program product in accordance with Claim 47 wherein said connection address table contains multiple IP bearer path entries having associated tuples identifying said first IP endpoint, and further including program means for implementing a bearer path pivot point by selectively activating the status flags associated with said IP bearer path entries.

50. A program product in accordance with Claim 41 further including program means for relaying signaling messages from one of said IP endpoints to a destination.

51. A program product in accordance with Claim 50 wherein said signaling message relaying program means includes program means for maintaining an IP endpoint address table that lists IP addresses for IP endpoints that are authorized to send signaling messages to said destination, and which lists IP PAG port numbers, one for each said IP endpoint.

52. A program product in accordance with Claim 51 wherein said signaling message relay program means includes program means for receiving a signaling traffic IP packet from said first or second IP endpoint and rewriting the packet header of said signaling packet by:

setting the source IP address to said IP address associated with said IP PAG relaying said signaling messages;

setting the source port number to said port number assigned to said IP endpoint, as determined from said IP endpoint address table;

setting the destination IP address to an IP address of said destination, as determined by the source IP address and destination port number of signaling message received; and

leaving the destination IP port unchanged.

53. A program product in accordance with Claim 52 wherein said signaling message is an H.323, SIP, or H.248 signaling message and said destination is a call control entity.

54. A program product in accordance with Claim 52 wherein said signaling message is an SNMP signaling message and said destination is an SNMP manager.

55. A program product in accordance with Claim 52 wherein said signaling message relay program means includes program means for performing signaling traffic policing to verify that said IP endpoint sending said signaling messages is authorized to send such messages.

56. A program product in accordance with Claim 55 wherein said signaling traffic policing program means includes program means for performing a table lookup in said IP endpoint address table relative to an IP signaling packet received from said first IP endpoint to verify that said IP endpoint is listed in said table and to obtain a port number assigned to said IP endpoint from said table.

57. A program product in accordance with Claim 55 further including program means for dynamically throttling signaling messages sent to said destination.

58. A program product in accordance with Claim 41 including program means for terminating plural IP lines at a set of line-side terminating points and terminating plural IP trunks at a set of trunk-side terminating points.

59. A program product in accordance with Claim 58 further including program means for performing switching between said line-side and trunk-side terminating points.

60. A program product in accordance with Claim 59 further including program means for connecting one of more of said line-side or trunk side terminating points to one or more resource servers, interworking gateways, interworking units, or data termination systems.